

Phishing and Pharming: Helping Consumers Avoid Internet Fraud

provided by: <http://www.bos.frb.org/consumer>



Gone are the days when we had to step outside to purchase our groceries, book flights and vacations, rent or purchase cars, or just transfer money between bank accounts. Today, we can simply grab our checkbooks, debit cards or credit cards, sit down at a computer in the comfort and safety of our home, and complete these transactions with passwords and PIN numbers. Thanks to advances in technology, the types of transactions we can now complete online are virtually endless. Unfortunately, the increase in online transactions has been accompanied by an increase in online identity theft. Fraudulent access to personal information over the Internet is increasingly prevalent and sophisticated. Two forms of identity theft are at the forefront of this Internet piracy: PHISHING and PHARMING.

Identity theft is a federal crime. It occurs when one person's identification (which can include name, social security number, bank account number, or any other account number) is used or transferred by another person for unlawful activities.

THE CRIME

PHISHING is a form of online identity theft that lures consumers into divulging their personal financial information to fraudulent web sites, also known as spoofed web sites. For example, the phisher sends an email message to an unsuspecting victim instructing him to click on the link to a bank's web site (provided in the email) to confirm his account information. Unbeknownst to the consumer, the web site is a convincing fake or copy of the authentic web site. The unsuspecting customer takes the bait and provides the information, thereby enabling the phisher to steal his personal financial information. The phisher can then use this information to clean out the victim's bank accounts or commit other forms of identity theft.

PHARMING is similar to phishing but more sophisticated. Pharmers also send emails. The consumer, however, can be duped by the pharmer without even opening an email attachment. The consumer compromises his personal financial information simply by opening the email message. The pharming email message contains a virus (or Trojan horse) that installs a small software program on the user's computer. Subsequently, when the consumer tries to visit an official web site, the pharmer's software program redirects the browser to the pharmer's fake version of the web site. In this way, the pharmer is able to capture the personal financial information that the consumer enters into the counterfeit web site, and the consumer's account is again compromised. The latest form of pharming does not require email at all. Password-stealing Trojan horses can attack through Microsoft Messenger® where keyloggers are run. Keyloggers are viruses that track a user's keystrokes on legitimate sites and steal passwords, allowing a thief to have access to a consumer's password for future fraudulent transactions.

THE SOLUTION

Consumer awareness is the key to avoid falling prey to phishers and pharmers. Ask representatives of your financial institution if they have implemented any special software to thwart off these identity thieves. Inquire as to whether your home PC software provider offers any updated anti-phishing programs. In addition, the Anti-Phishing Working Group (an association focused on eliminating the fraud and identity theft that result from phishing, pharming, and email spoofing) offers the following suggestions to avoid falling victim to an Internet scheme:

- Be suspicious of any email with urgent requests for personal financial information.
- Do not use the links in an email to get to any web page.
- Avoid completing forms in email messages that ask for personal financial information.

- Be sure to use a secure web site when submitting credit card or other sensitive information via the web browser.
- Consider installing a web browser tool bar for protection from known phishing fraud web sites.
- Regularly log on to online accounts.
- Regularly check bank, credit card, and debit card statements to ensure all transactions are legitimate.
- Make sure your browser is up to date and security patches are applied.

Be vigilant about protecting yourself from these newer forms of identity theft. When turning on your home computer to complete seemingly simple transactions, keep your eyes and ears open to avoid financial and emotional distress. If you have received a spoofed email message or believe that you have been a victim of phishing or pharming, there are steps you can take to help shut down the phisher, pharmer, or spoofer:

- Forward the email to the Federal Trade Commission at spam@uce.gov
- Forward the email to the "abuse" email address at the company that is being spoofed (e.g. spoof@ebay.com)
- Notify the Internet Fraud Complaint Center (IFCC) of the FBI by filing a complaint on the IFCC's web site: www.ifccfbi.gov

When forwarding email, always include the entire original email.